MRD Rank Metric Convolutional Codes

Diego Napp*, Raquel Pinto*, Joachim Rosenthal†, and Paolo Vettori*
*Department of Mathematics, University of Aveiro
3810-197 Aveiro, Portugal
Email: {diego,raquel,pvettori} at ua.pt
†Department of Mathematics, University of Zurich
Winterthurstrasse 190, CH-8057 Zürich, Switzerland
Email: rosenthal at math.uzh.ch

***Abstract*—So far, in the area of Random Linear Network Coding, attention has been given to the so-called one-shot network coding, meaning that the network is used just once to propagate the information. In contrast, one can use the network more than once to spread redundancy over different shots. In this paper, we propose rank metric convolutional codes for this purpose. The framework we present is slightly more general than the one which can be found in the literature. We introduce a rank distance, which is suitable for convolutional codes, and derive a new Singleton-like upper bound. Codes achieving this bound are called Maximum Rank Distance (MRD) convolutional codes. Finally, we prove that this bound is optimal by showing a concrete construction of a family of MRD convolutional codes.**

I. Introduction

Random Linear Network Coding (RLNC), as introduced in [1], provides the mathematical foundation for multicast communications and, in particular, for networks with unknown or changing topology. In this scenario, networks operate with packets. If one considers a packet as a row of a matrix with entries in a finite field, then the linear combinations performed in the nodes are row operations on this matrix. For perfect communications, the row space of the transmitted matrix remains unchanged. RLNC has since then opened a major research area in communications with widespread applications to wireless networks, internet or cloud computing. Most of the large body of literature in this area is concerned with the so-called *one-shot* network coding, meaning that the unknown structure of the network is used once to disseminate the information.

As opposed to this situation, coding can also be performed over multiple uses of the network, whose internal structure may change at each shot, giving rise to the so-called *multi-shot coding*. In fact, it has been recently shown that spreading redundancy among the transmitted codewords (row spaces) at different instances (shots) can improve the error-correction capabilities of the code [2]–[4].

To this end, in this work we propose to use rank metric convolutional codes, as this class of codes allows to create dependencies between data streams in a quite simple way. In this setting, an extension of the standard rank metric over multiple shots, which is analogous to the *extended subspace distance* defined in [2], will provide the proper measure for the number of rank erasures that a code can tolerate. We point out that this more involved multi-shot framework has proven to cope with network streaming applications with tight latency constrains (see [4] and the references therein).

The framework presented in this paper is slightly more general than the existing one in the literature on rank metric convolutional codes, which is mainly based (see [3], [4]) on rank metric Gabidulin codes [7]. Indeed, as proposed in [8], we shall define rank metric codes for all rates and fields.

In this contribution, we aim to further explore this approach. Specifically, after recalling some basic facts about convolutional and rank metric codes, we introduce a first general definition of rank metric convolutional codes, we propose a suitable concept of distance, and we study the Singleton-like bound for this class of codes. To conclude, we provide a family of rank metric convolutional codes, by direct construction, which achives the Singleton bound.

Notation

Following the traditional setting of Coding Theory, vectors over some ring R will be represented as rows. Moreover, to simplify some formulas and to maintain the correspondence with powers of polynomials, indices of vector and matrices will start from zero. So, for instance $v \in R^n$ will be written componentwise, as $v = (v_0, \ldots, v_{n-1})$ or $v = [v_0 \cdots v_{n-1}]$. For analogous reasons, $0 \in \mathbb{N}$.

For the sake of simplicity, the R-isomorphism $R^{n\times m} \to R^{mn}$ will be often exemplified by the map rowvec$: M \mapsto v$, such that $v_{mi+j} = M_{i,j}$, with $0 \leq i < n$ and $0 \leq j < m$. Note that, denoting by vec the standard vectorization of a matrix, which stacks its columns into a column vector, then $\text{rowvec}(M) = \text{vec}(M^\top)^\top$.

The inverse of the rowvec map will be denoted by rowmat or $\text{rowmat}_{n\times m}$, folding an mn (row) vector into an $n \times m$ matrix.

II. Convolutional Codes

Let $\mathbb{F}_q$ be a finite field and $\mathbb{F}_q[D]$ be the ring of polynomials with coefficients in $\mathbb{F}_q$. A *convolutional code* $\mathscr{C}$ of rate k/n is

*This work was supported in part by the Portuguese Foundation for Science and Technology (FCT-Fundação para a Ciência e a Tecnologia), through CIDMA - Center for Research and Development in Mathematics and Applications, within project UID/MAT/04106/2013.

†Partially supported by the the Swiss National Science Foundation under grant no. 169510.

a rank k $\mathbb{F}_q[D]$-submodule of $\mathbb{F}_q[D]^n$. If $G(D) \in \mathbb{F}_q[D]^{k\times n}$ is a full row rank matrix such that

$$\mathscr{C} = \mathrm{Im}_{\mathbb{F}_q[D]}\, G(D) = \left\{ u(D)G(D) : u(D) \in \mathbb{F}_q[D]^k \right\},$$

then $G(D)$ is called an *encoder* of $\mathscr{C}$.

Any other encoder $\tilde{G}(D)$ of $\mathscr{C}$ differs from $G(D)$ by a unimodular matrix $U(D) \in \mathbb{F}_q[D]^{k\times k}$, i.e., $\tilde{G}(D) = U(D)G(D)$. Therefore, we can consider $G(D)$ to be *minimal*, i.e., in row reduced form.[1] In this case, the sum of the row degrees of $G(D)$ attains its minimum among all the encoders of $\mathscr{C}$, which is usually denoted by δ and called the *degree* of $\mathscr{C}$.

A rate k/n convolutional code $\mathscr{C}$ of degree δ is called an (n,k,δ) convolutional code [5].

An important distance measure for a convolutional code $\mathscr{C}$ is its *free distance* $d_{\text{free}}(\mathscr{C})$ defined as

$$d_{\text{free}}(\mathscr{C}) = \min_{v(D)\in\mathscr{C}, v(D)\neq 0} \mathrm{wt}\big(v(D)\big),$$

where $\mathrm{wt}\big(v(D)\big)$ is the Hamming weight of a polynomial vector

$$v(D) = \sum_{i\in\mathbb{N}} v_i D^i \in \mathbb{F}_q[D]^n,$$

defined as

$$\mathrm{wt}\big(v(D)\big) = \sum_{i\in\mathbb{N}} \mathrm{wt}(v_i),$$

being $\mathrm{wt}(v_i)$ the number of the nonzero components of v_i.

In [6], Rosenthal and Smarandache showed that the free distance of an (n,k,δ) convolutional code is upper bounded by

$$d_{\text{free}}(\mathscr{C}) \leq (n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta + 1.$$

This bound was called the *generalized Singleton bound* since it generalizes in a natural way the Singleton bound for block codes (when $\delta = 0$). An (n,k,δ) convolutional code whose free distance is equal to the generalized Singleton bound is called *maximum distance separable* (MDS) code [6].

III. Rank Metric Codes

Let $A, B \in \mathbb{F}_q^{n\times m}$. It is known [7] that

$$d_{\text{rank}}(A,B) = \mathrm{rank}(A-B) \tag{1}$$

defines a distance, called *rank distance*, between A and B. Therefore, any subset of $\mathbb{F}_q^{n\times m}$ equipped with this distance is a rank metric code.

In particular, an $(n\times m,k)$ *linear rank metric code* $\mathscr{C} \subset \mathbb{F}_q^{n\times m}$ of rate $k/nm < 1$ is the image of a monomorphism $\varphi : \mathbb{F}_q^k \to \mathbb{F}_q^{n\times m}$. We write $\varphi = \psi \circ \gamma$ as a composition of an isomorphism ψ and a monomorphism γ:

$$\begin{array}{ccccc} \varphi : \mathbb{F}_q^k & \xrightarrow{\gamma} & \mathbb{F}_q^{nm} & \xrightarrow{\psi} & \mathbb{F}_q^{n\times m} \\ u & \longmapsto & v = uG & \longmapsto & V = \psi(v) \end{array}$$

[1] The polynomial matrix $G(D) \in \mathbb{F}_q[D]^{k\times n}$ is in row reduced form if it has a full row rank *leading row coefficient matrix* G_{lrc}, whose entries are the coefficients of the powers with highest degree (called *row degree*) in each row of G.

where $G \in \mathbb{F}_q^{k\times nm}$. If $\psi = \mathrm{rowmat}_{n\times m}$, the rows of V are simply the n consecutive blocks with m elements of v.

As usual, the rank distance of the code, $d_{\text{rank}}(\mathscr{C})$, is the minimum distance between nonzero codewords.

In the following, we will assume that $n \leq m$ (but analogous results can be given for the other case). Also for this class of codes, a Singleton-like bound exists, which provides a limit for the value of the code distance.

Theorem 1. *The rank distance of an $(n\times m,k)$ linear rank metric code is upper bounded by*

$$d_{\text{rank}}(\mathscr{C}) \leq n - \left\lfloor \frac{k-1}{m} \right\rfloor = n - \left\lceil \frac{k}{m} \right\rceil + 1.$$

Proof: It follows directly from the fact (see for instance [7]) that

$$log_q|\mathscr{C}| \leq \max\{n,m\}(\min\{n,m\} - d_{\text{rank}}(\mathscr{C}) + 1).$$

■

IV. Rank Metric Convolutional Codes

In this section we will define rank metric convolutional codes whose codewords are polynomials matrices in $\mathbb{F}_q[D]^{n\times m}$.

The *rank weight* of a polynomial matrix $A(D) = \sum_{i\in\mathbb{N}} A_i D^i \in \mathbb{F}_q[D]^{n\times m}$, is given by

$$\mathrm{rkwt}\big(A(D)\big) = \sum_{i\in\mathbb{N}} \mathrm{rank} A_i. \tag{2}$$

If $B(D) = \sum_{i\in\mathbb{N}} B_i \in \mathbb{F}_q[D]^{n\times m}$, we define the *sum rank distance* between $A(D)$ and $B(D)$ as

$$\begin{aligned} d_{\text{SR}}\big(A(D),B(D)\big) &= \mathrm{rkwt}\big(A(D)-B(D)\big) \\ &= \sum_{i\in\mathbb{N}} \mathrm{rank}(A_i - B_i). \end{aligned} \tag{3}$$

Lemma 2. *The sum rank distance d_{SR} is a distance in $\mathbb{F}_q[D]^{n\times m}$.*

Proof: Obviously $d_{\text{SR}}(A(D),B(D)) = d_{\text{SR}}(B(D),A(D))$ and $d_{\text{SR}}(A(D),B(D)) \geq 0$ with $d_{\text{SR}}(A(D),B(D)) = 0$ iff $A(D) = B(D)$. Further, as $\mathrm{rank}(X+Y) \leq \mathrm{rank}(X) + \mathrm{rank}(Y)$ for any $X, Y \in \mathbb{F}_q^{n\times m}$, then the triangular inequality readily follows,

$$\begin{aligned} d_{\text{SR}}\big(A(D),B(D)\big) &= \sum_{i\in\mathbb{N}} \mathrm{rank}(A_i - B_i) \\ &\leq \sum_{i\in\mathbb{N}} \mathrm{rank}(A_i - C_i) + \mathrm{rank}(C_i - B_i) \\ &= d_{\text{SR}}(A(D),C(D)) + d_{\text{SR}}(C(D),B(D)), \end{aligned}$$

for any $C(D) = \sum_{i\in\mathbb{N}} C_i D^i \in \mathbb{F}_q[D]^{n\times m}$. ■

A *rank metric convolutional code* $\mathscr{C} \subset \mathbb{F}_q^{n\times m}$ is the image of an homomorphism $\varphi : \mathbb{F}_q[D]^k \to \mathbb{F}_q[D]^{n\times m}$. We write $\varphi = \psi \circ \gamma$ as a composition of a monomorphism γ and an isomorphism ψ:

$$\begin{array}{ccccc} \varphi : \mathbb{F}_q[D]^k & \xrightarrow{\gamma} & \mathbb{F}_q[D]^{nm} & \xrightarrow{\psi} & \mathbb{F}_q[D]^{n\times m} \\ u(D) & \mapsto & v(D) = u(D)G(D) & \mapsto & V(D) \end{array} \tag{4}$$

where $G(D) \in \mathbb{F}_q^{k\times nm}$ is a full row rank polynomial matrix, called *encoder* of $\mathscr{C}$, and we may choose, as before, $V(D) = \text{rowmat}_{n\times m}\big(v(D)\big)$, such that $V_{i,j}(D) = v_{mi+j}(D)$.

As for convolutional codes, two encoders of $\mathscr{C}$ differ by left multiplication by a unimodular matrix and therefore $\mathscr{C}$ always admits minimal encoders (i.e., in row reduced form). The degree of a rank metric convolutional code $\mathscr{C}$ is the sum of the row degrees of a minimal encoder of $\mathscr{C}$, i.e. the minimum value of the sum of the row degrees of its encoders.

A rank metric convolutional code $\mathscr{C}$ of degree δ, defined as in (4), is called an $(n\times m,k,\delta)$-rank metric convolutional code.

The *sum rank distance* of a rank metric convolutional code $\mathscr{C}$ is defined as

$$\begin{aligned} d_{\text{SR}}(\mathscr{C}) &= \min_{V(D),U(D)\in\mathscr{C},V(D)\neq U(D)} d_{\text{SR}}(V(D),U(D)) \\ &= \min_{0\neq V(D)\in\mathscr{C}} \text{rkwt}\big(V(D)\big). \end{aligned}$$

Next theorem, which establishes the Singleton-like bound for rank metric convolutional codes, can be found in [8]. We present its proof for completeness.

Theorem 3. *Let $\mathscr{C}$ be an $(n\times m,k,\delta)$-rank metric convolutional code. Then the sum rank distance of $\mathscr{C}$ is upper bounded by*

$$d_{\text{SR}}(\mathscr{C}) \le n\left(\left\lfloor\frac{\delta}{k}\right\rfloor+1\right) - \left\lceil\frac{k(\left\lfloor\frac{\delta}{k}\right\rfloor+1)-\delta}{m}\right\rceil + 1. \tag{5}$$

Proof: Let $G(D)$ be a minimal encoder of $\mathscr{C}$ with row degrees $\nu_0,\nu_1,\ldots,\nu_{k-1}$. Let $\nu = \min\{\nu_i : 0\le i<k\}$ denote the value of the smallest row degree and t the number of indexes ν_i among the indexes $\nu_0,\nu_1,\ldots,\nu_{k-1}$ having the value ν. We shall assume, without loss of generality, that the row degrees of $G(D)$ are in nonincreasing order, i.e.,

$$\nu_0 \ge \cdots \ge \nu_{k-t-1} > \nu_{k-t} = \cdots = \nu_{k-1} = \nu$$

and that $\psi = \text{rowmat}_{n\times m}$ in (4).

Now take a nonzero and constant $u(D) = u = (0,\ldots,0,u_{k-t},\ldots,u_{k-1}) \in \mathbb{F}_q^k$: note that, due to this choice of $u(D)$, the degree of $v(D) = u(D)G(D)$ goes up to ν and not to ν_0, being $v(D) = v_0 + v_1D + v_2D^2 + \cdots + v_\nu D^\nu$. Denote $V(D) = \psi\big(v(D)\big) = V_0 + V_1D + \cdots + V_\nu D^\nu$. Observe that $v_0 = uG(0)$ is a linear combination of the last t rows of $G(0)$, thus we can select $u_{k-t},\ldots,u_{k-1}$ such that the first $t-1$ components of v_0 are zero. Therefore, also the first $\lfloor\frac{t-1}{m}\rfloor$ rows of $V_0 = \psi(v_0)$ are zero, which implies that $\text{rank}(V_0) \le n - \lfloor\frac{t-1}{m}\rfloor = n - \lceil\frac{t}{m}\rceil + 1$. Thus,

$$\begin{aligned} \text{rank}(V(D)) &= \sum_{0\le i\le\nu} \text{rank}(V_i) \\ &\le n - \left\lceil\frac{t}{m}\right\rceil + 1 + n\nu \\ &= n(\nu+1) - \left\lceil\frac{t}{m}\right\rceil + 1. \end{aligned}$$

This upper bound is maximized when ν is as large as possible and t as small as possible. It can be checked that, for given k and $\delta = \sum_{0\le i<k}\nu_i$, these values are $\nu = \lfloor\frac{\delta}{k}\rfloor$ and $t = k\left(\lfloor\frac{\delta}{k}\rfloor+1\right) - \delta$. This concludes the proof. ∎

A rank metric convolutional code whose distance attains the upper bound (5) is called *maximum rank distance* (MRD) convolutional code. Next corollary gives a necessary condition on the rows of a minimal encoder of a rank metric convolutional code $\mathscr{C}$ so it can be MRD, and it follows immediately from the proof of Theorem 3.

Corollary 4. *Let $\mathscr{C}$ be a $(n\times m,k,\delta)$-rank metric convolutional code and $G(D)\in\mathbb{F}_q$ a minimal encoder of $\mathscr{C}$. Then if $\mathscr{C}$ is MRD, $G(D)$ must have $k(\lfloor\frac{\delta}{k}\rfloor+1)-\delta$ rows of degree $\lfloor\frac{\delta}{k}\rfloor$ and $\delta - k\lfloor\frac{\delta}{k}\rfloor$ rows of degree $\lfloor\frac{\delta}{k}\rfloor+1$.*

V. Construction of MRD Convolutional Codes

In this section we will show that MRD rank metric convolutional codes exist, thus proving that bound (5) is optimal. We begin considering a simple particular case, which may help to understand the following general construction.

Let $\mathbb{F}_q$ be a finite field and $A\in\mathbb{F}_q^{m\times m}$ a matrix with irreducible characteristic polynomial $\chi(\lambda)$. Note that A^i, $0\le i<m$, are linearly independent over $\mathbb{F}_q$ and

$$\mathbb{F}_q[A] = \left\{\sum_{i=0}^{m-1} u_iA^i : u_i\in\mathbb{F}_q, i=0,\ldots,m-1\right\} \cong \mathbb{F}_{q^m} \tag{6}$$

is a field.

We will prove that, whenever $m>\delta$, the $(m\times m,1,\delta)$-rank metric convolutional code $\mathscr{C}$ generated by

$$G(D) = \sum_{i=0}^{\delta} \psi^{-1}(A^i)D^i \in \mathbb{F}_q[D]^{1\times m^2} \tag{7}$$

is MRD. In other words, its sum rank distance achieves the upper bound (5) given in Theorem 3, which in this case is equal to $m(\delta+1)$.

Actually, we will show that for any nonzero $u(D)\in\mathbb{F}_q[D]$ the codeword $V(D) = \varphi\big(u(D)\big)$ has rank weight $\text{rkwt}\big(V(D)\big) \ge m(\delta+1)$.

Let $u(D) = \sum_{i\in\mathbb{N}} u_iD^i$ be a nonzero polynomial. Without loss of generality, we may suppose that $u_0\neq 0$. Then, the first $\delta+1$ coefficients of $v(D) = \gamma\big(u(D)\big) = u(D)G(D)$ are thus given by

$$\begin{aligned} v_i &= \sum_{l=0}^{i} u_{i-l}G_l = \sum_{l=0}^{i} u_{i-l}\psi^{-1}(A^l) \\ &= \psi^{-1}\left(\sum_{l=0}^{i} u_{i-l}A^l\right),\ i\le\delta, \end{aligned}$$

due to linearity of ψ^{-1}. It follows that the polynomial matrix $V(D) = \psi\big(v(D)\big)$ has coefficients

$$\begin{aligned} V_i = \psi(v_i) &= \psi\left(\psi^{-1}\left(\sum_{l=0}^{i} u_{i-l}A^l\right)\right) \\ &= \sum_{l=0}^{i} u_{i-l}A^l \in \mathbb{F}_q[A],\ i\le\delta. \end{aligned} \tag{8}$$

Since the powers of A with degree less than m form a basis of $\mathbb{F}_q[A]$ over $\mathbb{F}_q$ and the scalar $u_0 \neq 0$ shows up in every linear combination, then $V_i \neq 0$ for every $i \leq \delta < m$. Being elements of a field, nonzero matrices are invertible and so have rank m. Therefore,

$$\operatorname{rkwt}\big(V(D)\big) = \sum_{i\in\mathbb{N}} \operatorname{rank} V_i \geq \sum_{i=0}^{\delta} \operatorname{rank} V_i = m(\delta+1). \tag{9}$$

Next example illustrates the reasoning above.

Example 5. *Consider the companion matrix A of the irreducible polynomial $\chi(\lambda) = \lambda^3 + \lambda + 1 \in \mathbb{F}_2[\lambda]$,*

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \in \mathbb{F}_2^{3\times 3}$$

and the rank metric convolutional code $\mathscr{C}$ with encoder $G(D) = \psi^{-1}(I) + \psi^{-1}(A)D = \psi^{-1}(I+AD) \in \mathbb{F}_2[D]^{1\times 9}$.

For the sake of simplicity, let $\psi = \operatorname{rowmat}_{m\times m}$ (folding a row vector into a matrix), thus ψ^{-1} is the 'rowvec' *map (unfolding a matrix into a row vector). This means that*

$$G(D) = \left[\begin{array}{ccc|ccc|ccc} 1 & D & 0 & 0 & 1 & D & D & D & 1 \end{array}\right].$$

Since $m = 3 > \delta = 1$, it follows that $\mathscr{C}$ is an MRD $(3\times 3, 1, 1)$-rank metric convolutional code, with distance equal to the upper bound (5)*, i.e., $d_{\mathrm{SR}}(\mathscr{C}) = m(\delta+1) = 6$, as we will show.*

Observe that, due to the rather simple structure of the code, its codewords are

$$\begin{aligned} V(D) &= \varphi\big(u(D)\big) = \psi\big(u(D)G(D)\big) \\ &= u(D)\psi\big(G(D)\big) = u(D)(I+AD). \end{aligned}$$

Furthermore, notice that any message starting with a nonzero coefficient is equal either to (a) $u(D) = 1 + \tilde{u}(D)D^2$ or to (b) $u(D) = 1 + D + \tilde{u}(D)D^2$, for some $\tilde{u}(D) \in \mathbb{F}_2[D]$.

As a consequence, every codeword in $\mathscr{C}$ must be of the form

$$V(D) = \big(1 + \tilde{u}(D)D^2\big)(I+AD) = I + AD + \tilde{V}(D)D^2 \tag{a}$$

or of the form

$$\begin{aligned} V(D) &= \big(1 + D + \tilde{u}(D)D^2\big)(I+AD) \\ &= I + (I+A)D + \tilde{V}(D)D^2, \end{aligned} \tag{b}$$

for some $\tilde{V}(D) \in \mathbb{F}_2[D]^{3\times 3}$. So, since in both cases the first two coefficients of $V(D)$ ($V_0 = I$ and $V_1 = A$ or $V_1 = I + A = A^3$) are nonzero, thus full rank matrices (invertible in the field $\mathbb{F}_2[A]$), the rank weight of any codeword of $\mathscr{C}$ is

$$\operatorname{rkwt}\big(V(D)\big) = \operatorname{rank} V_0 + \operatorname{rank} V_1 + \operatorname{rkwt}\big(\tilde{V}(D)\big) \geq 6.$$

For the general construction of an MRD $(n\times m, k, \delta)$-rank metric convolutional code over $\mathbb{F}_q$, with $m \geq n$, we still need a matrix $A \in \mathbb{F}_q^{m\times m}$ with irreducible characteristic polynomial. Moreover, let $X \in \mathbb{F}_q^{n\times m}$ be any full row rank matrix and define the $k \times nm$ matrices

$$G_i = \begin{bmatrix} \psi^{-1}(XA^{ki}) \\ \psi^{-1}(XA^{ki+1}) \\ \vdots \\ \psi^{-1}(XA^{ki+k-1}) \end{bmatrix}, \; 0 \leq i \leq \left\lfloor \frac{\delta}{k} \right\rfloor, \text{ and}$$

$$G_{\left\lfloor \frac{\delta}{k} \right\rfloor + 1} = \begin{cases} 0 & \text{if } k \text{ divides } \delta, \\ \begin{bmatrix} \psi^{-1}(XA^{k\left\lfloor \frac{\delta}{k} \right\rfloor + k}) \\ \vdots \\ \psi^{-1}(XA^{k+\delta-1}) \\ 0 \\ \vdots \\ 0 \end{bmatrix} & \text{otherwise.} \end{cases} \tag{10}$$

Theorem 6. *The $(n\times m, k, \delta)$-rank metric convolutional code $\mathscr{C}$, with encoder*

$$G(D) = \sum_{i=0}^{\left\lfloor \frac{\delta}{k} \right\rfloor + 1} G_i D^i \in \mathbb{F}_q[D]^{k\times nm}, \tag{11}$$

whose coefficients are defined in (10)*, is MRD when $m \geq \delta + k$.*

Proof: First of all, observe that Theorem 3 gives in this case the upper bound

$$d_{\mathrm{SR}}(\mathscr{C}) \leq n\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right). \tag{12}$$

Actually, note that $r = \delta - k\left\lfloor \frac{\delta}{k} \right\rfloor$ is the remainder of the integer division of δ by k, being $0 \leq r < k$. Therefore, $0 < k - r = k\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) - \delta \leq k$. By hypothesis, $m \geq \delta + k$, and therefore it follows that $0 < \frac{k\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) - \delta}{m} \leq 1$ for every $\delta \geq 0$. This shows that $\left\lceil \frac{k\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) - \delta}{m} \right\rceil = 1$, thus proving (12).

Consider now any message $u(D) = \sum_{i\in\mathbb{N}} u_i D^i \in \mathbb{F}_q[D]^k$ having, without loss of generality, a nonzero constant term u_0. We will show that (12) is actually a *lower bound* for the rank weight of the codeword $V(D) = \sum_{i\in\mathbb{N}} V_i D^i = \varphi\big(u(D)\big)$.

Let $v(D) = \gamma\big(u(D)\big) = u(D)G(D) \in \mathbb{F}_q[D]^{k\times nm}$. Then, the first $\left\lfloor \frac{\delta}{k} \right\rfloor + 1$ (row) vector coefficients of $v(D)$ are $v_i = \sum_{h=0}^{i} u_{i-h} G_h$, $0 \leq i \leq \left\lfloor \frac{\delta}{k} \right\rfloor$. To carry out the proof, a more

detailed result is needed: if $u_i = (u_{i,0}, \dots, u_{i,k-1})$ then

$$\begin{aligned} v_i &= \sum_{h=0}^{i} u_{i-h} G_h = \sum_{h=0}^{i} \sum_{l=0}^{k-1} u_{i-h,l} \psi^{-1}(XA^{kh+l}) \\ &= \sum_{h=0}^{i} \sum_{l=kh}^{kh+k-1} u_{i-h,l-kh} \psi^{-1}(XA^{l}) \\ &= \sum_{h=0}^{i} \sum_{l=kh}^{kh+k-1} u_{i-\lfloor \frac{l}{k} \rfloor, l-k\lfloor \frac{l}{k} \rfloor} \psi^{-1}(XA^{l}) \\ &= \sum_{l=0}^{ki+k-1} u_{i-\lfloor \frac{l}{k} \rfloor, l-k\lfloor \frac{l}{k} \rfloor} \psi^{-1}(XA^{l}) \\ &= \psi^{-1}\left(X \sum_{l=0}^{ki+k-1} u_{i-\lfloor \frac{l}{k} \rfloor, l-k\lfloor \frac{l}{k} \rfloor} A^{l} \right) \\ &= \psi^{-1}(XB), \end{aligned}$$

where $B_i = \sum_{l=0}^{ki+k-1} u_{i-\lfloor \frac{l}{k} \rfloor, l-k\lfloor \frac{l}{k} \rfloor} A^l$.

Once $k\lfloor \frac{\delta}{k} \rfloor - 1 < \delta$ and, by hypothesis, $\delta + k \le m$, it follows that $k\lfloor \frac{\delta}{k} \rfloor + k - 1 < m$. Thus, for all $0 \le i \le \lfloor \frac{\delta}{k} \rfloor$, matrices B_i are linear combinations of some powers A^l with exponents $0 \le l < m$, which are therefore linearly independent over $\mathbb{F}_q$. In particular, since there exist nonzero components of u_0 (which appear in the defining expression of B_i for $l \ge ki$), then $B_i \neq 0$. So, being each $B_i \in \mathbb{F}_q[A]$ a nonzero element of a field, it is invertible, thus it has full rank m. By definition, $V(D) = \psi\big(v(D)\big)$, hence $V_i = \psi(v_i) = XB_i$ will have (full row) rank n for every $0 \le i \le \lfloor \frac{\delta}{k} \rfloor$. Finally, the rank weight of $V(D)$ is

$$\operatorname{rkwt}\big(V(D)\big) = \sum_{i \in \mathbb{N}} \operatorname{rank} V_i \ge \sum_{i=0}^{\lfloor \frac{\delta}{k} \rfloor} \operatorname{rank} V_i = n\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1 \right). \tag{13}$$

To conclude the proof, we check that code $\mathscr{C}$ has degree δ. Looking at the definition (11) of $G(D)$ and of its coefficients (10), it is quite clear that the leading row coefficient matrix G_{lrc} of $G(D)$ has the first $\delta - k\lfloor \frac{\delta}{k} \rfloor$ of $G_{\lfloor \frac{\delta}{k} \rfloor + 1}$ and the last $k(\lfloor \frac{\delta}{k} \rfloor + 1) - \delta$ rows of $G_{\lfloor \frac{\delta}{k} \rfloor}$. By the previous analysis, G_{lrc} has full row rank k and the sum of the row degrees is

$$\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1 \right) \left(\delta - k \left\lfloor \frac{\delta}{k} \right\rfloor \right) + \left\lfloor \frac{\delta}{k} \right\rfloor \left(k \left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1 \right) - \delta \right) = \delta.$$

■

Remark 7. *In our setup, a rank metric code is defined by the $\mathbb{F}_q[D]$-homomorphism $\varphi : \mathbb{F}_q[D]^k \to \mathbb{F}_q[D]^{n \times m}$, i.e., according to the decomposition* (4)*, by the generator matrix $G(D)$ and by the isomorphism ψ. However, notice that the construction presented in* (10) *and* (11) *characterizes the code in terms of the (constant) matrices A and X: even if the isomorphism ψ appears in the entries of $G(D)$, it is canceled out in the composition $\varphi = \psi \circ \gamma$, as the proof of Theorem 6 shows. Therefore, for this construction, the choice of ψ is completely arbitrary.*

Next example shows how to construct an MRD rank metric convolutional code with parameters $n < m$ and $k > 1$.

Example 8. *To construct a $(3 \times 4, 2, 2)$ code, using the proposed algorithm, matrices A and X have to be defined. Being arbitrary, we choose once more $\psi = \operatorname{rowmat}_{3\times 4}$ and $\psi^{-1} = \operatorname{rowvec}$.*

So, consider the companion matrix A of the irreducible polynomial $\chi(\lambda) = \lambda^4 + \lambda + 1 \in \mathbb{F}_2[\lambda]$ and the full row rank matrix $X = \begin{bmatrix} I_3 & 0_{3\times 1} \end{bmatrix}$, i.e.,

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix} \in \mathbb{F}_2^{4\times 4}, \quad X = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \in \mathbb{F}_2^{3\times 4}.$$

Easy calculations offer

$$XA = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, XA^2 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}, XA^3 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix},$$

whence, by (10)*, we get*

$$G_0 = \begin{bmatrix} \psi^{-1}(X) \\ \psi^{-1}(XA) \end{bmatrix} = \left[\begin{array}{cccc|cccc|cccc} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{array}\right]$$

$$G_1 = \begin{bmatrix} \psi^{-1}(XA^2) \\ \psi^{-1}(XA^3) \end{bmatrix} = \left[\begin{array}{cccc|cccc|cccc} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \end{array}\right].$$

Consequently, a generator matrix for the requested code is

$$G(D) = G_0 + G_1 D = \left[\begin{array}{cccc|cccc|cccc} 1 & 0 & D & 0 & 0 & 1 & 0 & D & D & D & 1 & 0 \\ 0 & 1 & 0 & D & D & D & 1 & 0 & 0 & D & D & 1 \end{array}\right].$$

Note that, if $u(D) = [u_0 \ u_1] + [u_2 \ u_3]D + \dots \in \mathbb{F}_2[D]^2$, then the first two coefficients of the codeword $V(D) = \varphi\big(u(D)\big)$ are

$$V_0 = X(u_0 I + u_1 A) \text{ and } V_1 = X(u_2 I + u_3 A + u_0 A^2 + u_1 A^3).$$

Both matrices have rank equal to 3 for any choice of u_0, u_1, u_2, and u_3, with at least u_0 or u_1 nonzero, confirming that the distance of the code is at least $3(\lfloor \frac{2}{2} \rfloor + 1) = 6$.

References

[1] R. Kötter and F. Kschischang, "Coding for errors and erasures in random network coding," *IEEE Trans. Inform. Theory*, vol. 54, no. 8, pp. 3579–3591, Aug. 2008. DOI: 10.1109/tit.2008.926449.

[2] R. Nóbrega and B. Uchoa-Filho, "Multishot codes for network coding using rank-metric codes," in *Wireless Network Coding Conference (WiNC), 2010 IEEE*, Jun. 2010, pp. 1–6. DOI: 10.1109/winc.2010.5507933.

[3] A. Wachter-Zeh, M. Stinner, and V. Sidorenko, "Convolutional codes in rank metric with application to random network coding," *IEEE Trans. Inform. Theory*, vol. 61, no. 6, pp. 3199–3213, Jun. 2015. DOI: 10.1109/tit.2015.2424930.

[4] R. Mahmood, "Rank metric convolutional codes with applications in network streaming," Master of Applied Science, Graduate Department of Electrical and Computer Engineering, University of Toronto, 2015. [Online]. Available: https://tspace.library.utoronto.ca/handle/1807/70480.

[5] R. J. McEliece, "The algebraic theory of convolutional codes," in *Handbook of Coding Theory*, V. Pless and W. Huffman, Eds., vol. 1, Amsterdam, The Netherlands: Elsevier Science Publishers, 1998, pp. 1065–1138.

[6] J. Rosenthal and R. Smarandache, "Maximum distance separable convolutional codes," *Appl. Algebra Engrg. Comm. Comput.*, vol. 10, no. 1, pp. 15–32, 1999.

[7] E. Gabidulin, "Theory of codes with maximum rank distance," *Probl. Inf. Transm.*, vol. 21, pp. 1–12, 1985.

[8] D. Napp, R. Pinto, J. Rosenthal, and P. Vettori, "Rank metric convolutional codes," in *Proceedings of the 22nd International Symposium on Mathematical Theory of Networks and Systems*, Jul. 2016, pp. 361–363. [Online]. Available: http://conservancy.umn.edu/handle/11299/181518.